«УТВЕРЖДАЮ»

Директор Федерального
государственного бюджетного
учреждения науки
«Институт системного
программирования им.
В.П. Иванникова РАН»

Академик РАН
Аветисян Арутюн Ишханович

«12» февраля 2021 г.

ОТЗЫВ

ведущей организации на диссертационную работу Мордвинова Дмитрия Александровича **«Автоматический вывод реляционных инвариантов для нелинейных дизъюнктов Хорна с ограничениями»**, представленную на соискание учёной степени кандидата физико-математических наук по специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Актуальность темы диссертации. В последние десятилетия сложность практически используемых программных систем существенно увеличилась, и сегодня объем программного обеспечения, работающего на почти любом компьютере или смартфоне, составляет миллионы строк кода. В связи с этим серьезной проблемой становится обеспечение качества промышленного программного обеспечения, особенно с повышенными требованиями к надежности и безопасности. Наиболее высокую степень доверия при контроле качества имеют методы формальной верификации. В последние 15 лет они активно развиваются и расширяют область своей применимости, в частности, значительная часть компонентов широко используемых операционных систем уже проходит контроль с использованием этих методов. В рамках методов дедуктивной верификации одной из перспективных техник является использование индуктивных инвариантов для доказательства корректности программ. Индуктивные инварианты позволяют выразить свойства программ, которые верны для неограниченного множества путей исполнения программы, и вследствие этого широко применяются в автоматических и полуавтоматических верификаторах программного обеспечения. Однако, даже для простых программ описывающие их свойства инварианты могут оказаться довольно сложны, так что большинство эффективно разрешимых теорий

недостаточно выразительны для их представления с использованием только функциональных и предикатных символов самой программы. Эта проблема называется проблемой непредставимости инвариантов.

Дизъюнкты Хорна с ограничениями являются важным формализмом в контексте задачи вывода индуктивных инвариантов. С их помощью возможно моделировать различные свойства программ в виде набора логических импликаций, сводимых к дизъюнктам специального вида, и тогда проверка корректности программы сводится к проверке выполнимости этих дизъюнктов в некоторой теории, например, теории битовых векторов или теории массивов. Таким образом, в значительном числе случаев задача дедуктивной верификации программы может быть сведена к поиску символьного решения системы дизъюнктов Хорна с ограничениями, а сами символьные решения соответствует индуктивным инвариантам программы. Это позволяет использовать решатель дизъюнктов Хорна с ограничениями в качестве ядра верификатора. В 2010-х годах появилось множество решателей систем дизъюнктов Хорна — Spacer, Eldarica, HoIce, Qarmc и нек. др.

Однако существующие методы и решатели хорошо работают лишь в случае линейных систем дизъюнктов Хорна. Главная причина этого состоит в том, что проблема непредставимости индуктивных инвариантов проявляется преимущественно для нелинейных систем.

Диссертационная работа Мордвинова Д.А. «Автоматический вывод реляционных инвариантов для нелинейных дизъюнктов Хорна с ограничениями» относится к области верификации программного обеспечения и посвящена проблеме эффективного решения нелинейных систем дизъюнктов Хорна.

Предмет исследования – методы проверки выполнимости нелинейных систем дизъюнктов Хорна с ограничениями. Цель исследования включает в себя разработку и программную реализацию более эффективных, чем существующие, алгоритмов для такой проверки.

Основные полученные результаты

1. Предложен подход к синтаксической синхронизации систем дизъюнктов Хорна с ограничениями первого порядка, выполнено доказательство его корректности.
2. Создан алгоритм CHCproduct для реализации синхронизирующего преобразования дизъюнктов Хорна с ограничениями, представлено доказательство его корректности и завершаемости.
3. Введено понятие реляционного сертификата выполнимости, доказана теорема о том, что если у системы существует реляционный сертификат выполнимости, то она выполнима.
4. Создан алгоритм RelRecMc для автоматического построения реляционных сертификатов выполнимости систем дизъюнктов Хорна с ограничениями, доказана корректность алгоритма.
5. Выполнена реализация предложенных алгоритмов; также проведено экспериментальное исследование на тестовых примерах, включающих условия верификации свойств безопасности и реляционных проблем верификации свойств гипербезопасности, показавшее превосходство

предложенных алгоритмов по сравнению с существующими на нелинейных системах дизъюнктов Хорна.

Личный вклад. Размах решаемых в диссертации задач был достаточно большим и включал в себя, помимо формулировки алгоритмов и доказательства их корректности, значительный объем программирования (в том числе, встраивание предложенных алгоритмов в известный решатель Z3), а также проектирование и проведение экспериментов. Поэтому работа выполнялась коллективом под руководством автора. Мордвинову Д.А. принадлежат все основные идеи предлагаемого подхода, а также выполнение математических доказательств корректности и завершаемости алгоритмов. Соавторы помогали в реализации алгоритмов и экспериментов, а также участвовали в улучшениях доказательств и обсуждениях.

Новизна. Все результаты, выносимые на защиту, являются новыми. В работе было предложено синтаксическое преобразование дизъюнктов Хорна, которое позволило частично преодолеть проблему непредставимости символьных решений. Диссертант ввёл новое понятие реляционного сертификата выполнимости для нелинейных систем дизъюнктов Хорна, которое позволяет доказывать выполнимость нелинейных систем дизъюнктов Хорна во многих случаях, когда все символьные модели не представимы в языке ограничений. Также впервые был предложен алгоритм вывода реляционных сертификатов выполнимости для случая нелинейных систем дизъюнктов Хорна.

Теоретическая значимость. Предложенный метод синхронизации нелинейных систем дизъюнктов Хорна с ограничениями, а также понятие реляционного сертификата выполнимости позволяют доказывать выполнимость систем дизъюнктов Хорна с ограничениями даже в случаях, когда все символьные решения не представимы в языке ограничений. Это является частичным решением проблемы непредставимости символьных моделей систем дизъюнктов в языке ограничений, что существенно расширяет класс нелинейных задач в области верификации программ, которые могут решаться автоматически.

Практическая значимость работы заключается в предложении эффективного алгоритма решения нелинейных систем дизъюнктов Хорна с ограничениями. Дело в том, что на практике большинство значимых свойств о программах формулируются именно с помощью нелинейных систем. Кроме того, предложенный алгоритм был реализован в рамках известного SMT-решателя Z3, что открывает дорогу для практического применения созданного алгоритма, а также для его последующих дополнений и модификаций. Последнее обстоятельство (реализация в Z3) является одновременно и признанием практической важности результатов в международном сообществе (сейчас алгоритм диссертанта является официальной частью Z3), и возможностью для применения и дальнейшей эволюции подхода, в рамках которого он создан.

Обоснованность и достоверность научных выводов, положений и заключений подтверждена корректным использованием результатов современных исследований в области верификации и математической логики, применением математических методов доказательства, а также проведением экспериментов. Было проведено экспериментальное сравнение предложенных алгоритмов и наиболее эффективных на сегодняшний день решателей дизъюнктов Хорна с ограничениями на стандартно используемых для оценки таких решателей тестовых наборах. Его результаты позволяют однозначно утверждать, что разработанные методы существенно расширяют класс нелинейных проблем, решаемых автоматическими верификаторами, а также улучшение производительности по сравнению с существующими реализациями.

Экспериментальная проверка предлагаемых алгоритмов показала достоверность данных, приведённых в главе 5 диссертации. Встроенность реализаций в SMT-решатель Z3 позволила использовать стандартные входные и выходные форматы для спецификации тестовых проблем, что существенно упростило проверку корректности результатов.

Достоверность полученных результатов подтверждается также выступлениями на ведущих мировых конференциях по тематике LPAR, FMCAD, ECOOP, а также на семинарах в ведущих российских центрах – ИСП РАН, ИПМ РАН, ИСИ РАН, ВШЭ, МГУ.

Оценка содержания диссертационной работы, её завершенность в целом, замечания по оформлению

Диссертационное исследование Мордвинова Д.А. представляет собой содержательную, целостную работу, выполненную с привлечением самых последних методов исследования в области формальных методов дедуктивной верификации, в частности, методов поиска решений нелинейных дизъюнктов Хорна и PDR-подхода. Полученные автором результаты изложены внятно, последовательно и корректно.

В тексте диссертации не выявлено каких-либо противоречий. Предлагаемые методы решения сформулированных задач корректны, а задачи соответствуют цели работы.

Автор представил в работе аккуратное, но достаточно компактное описание основных понятий и методы предметной области, избежав чрезмерной детализации и излишнего погружения в основы. Формальные определения и формулировки обычно сопровождаются полезными неформальными пояснениями. Также каждая глава начинается с краткой аннотации ее содержания и заканчивается выводами и обсуждением полученных в ней результатов.

В **первой главе** дается введение в предметную область и сформулированы определения основных общеизвестных понятий, используемых в работе.

Во **второй главе** описывается метод синхронизации для приведения нелинейной системы дизъюнктов Хорна к линейному виду, сохраняющий как можно больше логических связей между неинтерпретированными символами. Продемонстрировано, что этот метод способен упростить нелинейную систему для инструментов автоматической проверки выполнимости, описаны границы

применимости, а также проиллюстрирована проблема экспоненциального роста числа правил в итоговой системе. Последующие главы посвящены, во многом, преодолению этой трудности.

В **третьей главе** введено понятие реляционных сертификатов выполнимости системы, которое помогает решать ту же проблему, что и метод синхронизации, но не посредством изменения системы, а посредством изменения вида решения этой системы. Наглядно продемонстрированы достоинства реляционных сертификатов. В частности, описан способ избегания экспоненциального роста числа правил посредством применения преобразования, напоминающего преобразование Цейтина.

В **четвертой главе** представлен алгоритм автоматического вывода реляционных сертификатов выполнимости.

В **пятой главе** представлены детали реализации алгоритма, а также результаты экспериментов с реализацией. Результаты представлены в нескольких таблицах и графиках, в удобном для восприятия виде.

Замечания

1. В ряде случаев автор даёт определения некоторых понятий прямо в тексте, не выделяя их в формальные определения. Это, однако, нигде не влияет на корректность и ясность изложения.
2. Иногда автор использует разные обозначения для одних и тех же понятий в различных частях текста диссертации. Это усложняет чтение работы.
3. В описании алгоритма RelBndSafety указано использование им неопределенной процедуры Partition для разбиения рекурсивных атомов, от свойств которой зависят важные свойства итогового алгоритма, в частности, его применимость к более широкому классу задач, чем у уже имеющихся подобных алгоритмов. Однако возможные реализации такой процедуры оставлены без пояснений, за исключением того, что тривиальная реализация в виде разбиения на одноэлементные множества атомов, приводит к обычным, не реляционным, сертификатам выполнимости, для получения которых имеются другие алгоритмы. Было бы полезно привести хотя бы какие-то примеры построения такой процедуры, приводящие на практике к расширению области применимости алгоритма на нелинейных системах.

Публикации в научной печати. Научные результаты, в полном объеме отражающие содержание диссертации, опубликованы в 7 печатных работах, из них: 2 статьи изданы в журналах из “Перечня рецензируемых научных изданий», формированного согласно требованиям, установленным Министерством образования и науки РФ, 3 статьи опубликованы в изданиях, индексируемых Scopus и Web of Science.

Заключение. Диссертационная работа Мордвинова Д.А. представляет собой законченное научное исследование, выполненное на высоком научном уровне. В работе получены результаты, являющиеся значимыми научными достижениями в области формальных методов дедуктивной верификации и верификации программного обеспечения.

Полученные автором диссертации результаты достоверны, выводы и заключения обоснованы.

Содержание диссертации полностью формуле специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей, и пунктами 1, 2, 5 паспорта специальности. Автореферат согласуется с диссертацией и полностью отражает ее основные положения.

Диссертационная работа соответствует критериям, установленным Положением о порядке присуждения учёных степеней, а её автор Мордвинов Дмитрий Александрович заслуживает присуждения ему учёной степени кандидата физико-математических наук по специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей.

Отзыв на диссертацию обсуждался и был утвержден на заседании семинара отдела «Технологий программирования» ИСП РАН 12 февраля 2021 года.

Отзыв составил
кандидат физико-математических наук, ведущий научный сотрудник Института системного программирования им. В. П. Иванникова РАН

Кулямин Виктор Вячеславович

телефон: (495) 9125317 д. 422
факс: (495) 9121524
e-mail: kuliamin@ispras.ru

Подпись Кулямина В. В. удостоверяю
Ученый секретарь Института системного программирования им. В. П. Иванникова РАН, кандидат технических наук

Самоваров Олег Ильгисович